REMARKS

In view of the following remarks, Applicant respectfully requests reconsideration and allowance of the subject application. This response is believed to be fully responsive to all issues raised in the June 17, 2005 Office Action.

Rejections to the Claims

35 U.S.C. 103(a)

Claims 1, 3, 4, 10, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,311,218 issued to Jain et al. (herein referred to as "Jain"), in view of U.S. Patent Number 6,725,276 issued to Hardjono et al. (herein referred to as "Hardjono"). Applicant respectfully traverses this rejection.

Applicant describes a user-authentication scheme in which a policy agent carries out a user-authentication process that authenticates the user who sends the network data and associates the network data received from the client computer with the authenticated user. In other words, the policy agent verifies that the user is indeed who they claim to be, and verifies that the received network data are indeed those sent by that user. (*Application*, page 10, lines 14 – 21.)

Specifically, claim 1 recites, in part:

> composing a challenge for authenticating a user of the client computer;
>
> decrypting the response ... to obtain a first message digest value;
>
> receiving network data through the network connection with the client computer; and
>
> calculating a second message digest value based on the challenge and the received network data.

The combination of Jain and Hardjono does not teach or suggest, "calculating a second message digest value based on the challenge and the received network data, " as recited in claim 1. The Office contends that Jain teaches decrypting a response to a challenge for authentication a user of the client computer to obtain a first message digest value, and that Hardjono teaches calculating a second message digest value based on the challenge and the received network data. Applicant respectfully disagrees, pointing out that Jain teaches a method of user authentication, and Hardjono teaches a method of domain authentication. However, neither Jain nor Hardjono, alone nor in combination, teach or suggest "calculating a second message digest value based on the challenge and the received network data," where the challenge is, "a challenge for authenticating a user of the client computer," as recited in claim 1.

Jain describes a user-authentication scheme based on a public/private encryption key, challenge/response mechanism. However, as agreed to by the Office (*Office Action*, page 4), Jain does not teach or suggest calculating a message digest value based on the challenge and the received network data.

Hardjono describes a system in which a border network device is implemented to enable transmission of messages between two distinct multicast domains. (*Hardjono*, Abstract.) Routers within each domain communicate via one or more messages that each has an appended tag known as a "Message Authentication Code" (MAC). The MAC is generated based on a symmetrical authentication key that is known to each router in the given domain. (Hardjono, column 5, lines 10-30). A message is considered to be "authentic" when received from an authorized network device within a given domain. (Hardjono, column 5, lines 43-45.)

When a message is transmitted from a router in the first domain to a router in the second domain, the sending router appends a MAC to the message, and transmits the message to a border router associated with the first domain. The border router associated with the first domain then cooperates with a border router associated with the second domain to translate the MAC to an appropriate MAC for the second domain. Once the MAC associated with the second domain is appended to the message, the message is transmitted to one or more receiving routers in the second domain. (*Hardjono*, Fig. 2, and column 5, line 56 – column 6, line 28.)

The tag that is appended to the message provides a means for authenticating that the message originated from a network device within the domain. The MAC described in Hardjono is used to authenticate that a message was received from a device within a particular network domain. Hardjono does not teach or suggest user authentication, and specifically, does not teach or suggest, calculating a second message digest value based on the challenge (for authenticating a user of the client computer) and the received network data.

A system implemented as a combination of the systems taught in Jain and Hardjono would perform one authentication to verify that network data being transmitted is being transmitted from a network device within a particular domain (as taught by Hardjono), and a second authentication to authenticate the identify of a user who supposedly sent the network data. However, the combination of Jain and Hardjono does not address the need for verifying that the user being authenticated actually sent the network data. For example, there may be a scenario in which a user may be authenticated to send data to a particular network device, but the authentication is based on the user identity – not a domain from which the user may send the data. In this case, given a system implemented based on the combined teachings of Jain and Hardjono, while the user may be authenticated (based on the teachings of Jain), the data may not be allowed to enter the network if the domain from which the user is attempting to send the data is not known to (and trusted by) the network. However, in a system implemented according to claim 1, if the user is authenticated and the data is successfully identified as having been sent by the user, then the network data may be allowed, regardless of a domain from which the data was sent.

Accordingly, for at least the reasons stated above, claim 1 is allowable over the combination of Jain and Hardjono.

Claims 3, 4, 10, and 11 are allowable by virtue of their dependency on claim 1.

Claims 2, 6-9, 13, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jain in view of Hardjono, and further in view of U.S. Patent Number 6,052,788 issued to Wesinger et al. (herein referred to as "Wesinger"). Applicant respectfully traverses this rejection.

Wesinger teaches a firewall that achieves maximum network security and maximum user convenience. The firewall employs "envoys" that exhibit the security robustness of prior-art proxies and the transparency and ease-of-use of prior-art packet filters, combining the best of both worlds. (*Wesinger*, abstract.) However, Applicant does not believe, nor does the Office contend that Wesinger adds anything to the teachings of Jain and Hardjono with regard to claim 1. Accordingly, claims 2, 6, and 7 are allowable by virtue of their dependency on claim 1. Furthermore, one or more of claims 2, 6, and 7 may also be allowable for other reasons. For example:

Claim 6 recites a computer-readable medium as in claim 1, wherein the received network data are in a form of packets, and the step of calculating calculates the second message digest value based on a pre-selected number of packets of the received network data.

The Office points to Wesinger column 4, lines 1-5 and column 10, lines 58-66 as teaching out-of-band authentication and network data packet filtering. The cited portions of Wesinger teach a user-authentication method and include a mention of content filtering, but the cited portions of Wesinger do not teach or suggest calculating "the second message digest value based on a pre-selected number of packets of the received network data," as recited in claim 6. Accordingly, and by virtue of its dependence on claim 1, claim 6 is allowable over the combination of Jain, Hardjono, and Wesinger.

Claim 8 recites elements similar to those recited in claim 1. The Office relies on Jain and Hardjono for teaching each of the elements recited in claim 8, and also mentions Wesinger, column 4, lines 1-5 and column 10, lines 58-66 as teaching an out-of-band authentication mechanism with reference to the claimed element of "generating, by the client computer, a first message digest value based on the network data of the user." As discussed above, the combination of Jain, Hardjono, and Wesinger does not teach or suggest a message digest value based on the network data of the user, as recited in claim 8. Accordingly, and for the same reasons stated above with reference to claim 1, claim 8 is allowable over the combination of Jain, Hardjono, and Wesinger.

Claims 9, 13, and 15 are allowable by virtue of their dependency on claim 8, and may also be allowable for other reasons, such as those stated above with reference to claim 7.

Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jain in view of Hardjono, and further in view of U.S. Patent Number 5,684,951 issued to Goldman et al. (herein referred to as "Goldman"). Applicant respectfully traverses this rejection.

Goldman teaches a method and system for performing user authorization in a multi-user computer system. When a user requests access to an application over the multi-user system, the application requires the user to input a user identification value and, simultaneously, the application accesses the user's current IP address. The application attempts to validate the user identification, and if valid, the application examines its database to determine if the user is authorized for its current IP address. (*Goldman*, abstract.) However, Applicant does not believe, nor does the Office contend that Goldman adds anything to the teachings of Jain and Hardjono with regard to claim 1. Accordingly, claim 5 is allowable by virtue of its dependency on claim 1.

Claims 12 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jain in view of Hardjono and Wesinger as applied to claim 8, and further in view of Goldman. Applicant respectfully traverses this rejection.

As described above with reference to claim 8, the combination of Jain, Hardjono, and Wesinger does not teach or suggest the elements recited in clam 8. Applicant does not believe, nor does the Office contend, that Goldman adds anything to the teachings of Jain, Hardjono, and Wesinger with regard to claim 8. Accordingly, claims 12 and 14 are allowable by virtue of their dependency on claim 8.

Conclusion

Claims 1-15 are believed to be in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the present application. Should any issue remain that prevents immediate issuance of the application, the Examiner is encouraged to contact the undersigned agent to discuss the unresolved issue.

Respectfully Submitted,
Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201

Dated: 10/17/05

Kayla D. Brant

Name: Kayla D. Brant
Reg. No. 46,576
Phone No. (509) 324-9256 ext. 242